



United States Council for International Business

1212 Avenue of the Americas, New York, NY 10036-1689
tel: 212-354-4480 ~ fax: 212-575-0327
e-mail: info@uscib.org ~ Internet: www.uscib.org

Serving American Business as U.S. Affiliate of:

International Chamber of Commerce (ICC)
International Organisation of Employers (IOE)
Business and Industry Advisory Committee (BIAC) to the OECD
ATA Carnet System

June 13, 2006

Mr. Eric Holloway
U.S. Department of Commerce
1401 Constitution Avenue, room 2806
Washington, DC 20230

Re: USCIB response to the Federal Register Notice on APEC Privacy Framework and Cross Border Privacy Rules

Dear Mr. Holloway,

The United States Council for International Business (USCIB) is pleased to provide comments on the Development and Implementation of Cross-border Privacy Rules in the Asia Pacific Cooperation Group as invited in the Federal Register Notice of May 22, 2006. USCIB and its members have been active in the development of the APEC Privacy Principles since the outset of this project. Our members have consistently argued that the greatest value-added of this APEC project would be the development of a mechanism to ensure transborder data flows throughout the APEC region through the establishment of a one-stop-shop approval process for corporate privacy practices for transborder information flows that comply with the APEC Principles. This response is an initial elaboration on such a process.

USCIB promotes an open system of global commerce in which business can flourish and contribute to economic growth, human welfare and protection of the environment. Its membership includes some 300 leading U.S. companies, professional services firms and associations whose combined annual revenues exceed \$3 trillion. As the exclusive American affiliate of three key global business groups – the International Chamber of Commerce, the International Organisation of Employers, and the Business and Industry Advisory Committee to the OECD – USCIB provides business views to policy makers and regulatory authorities worldwide, and works to facilitate international trade.

Cross border data transfers are vital to conducting business in a global economy. Much foreign direct investment is focused on services activities, such as providing access to 24x7 customer

service in a “following the sun” business model, and many countries are positioning themselves higher up the chain to more ‘value-added’ services output. The ability of countries to attract investment and nurture indigenous businesses will depend on them enabling the cross-border data flows on which the information economy depends. Differing government regulations on data transfers create impediments to the flow of information across borders that is the lifeblood of today's dynamic global economy. At the same time, the protection of an individual's personal information is an increasingly important issue around the world for governments, businesses and individuals.

The APEC Privacy Framework will help promote a consistent approach to privacy and accountability for cross-border information transfers across APEC member economies. It will ensure privacy protection while at the same avoiding unnecessary barriers to the free flow of information throughout the region that is so vital to the economic growth of the APEC region. The APEC Privacy Framework is important because it will enable companies to devise meaningful global privacy solutions for their cross-border data transactions.

Consumers, business, and governments all benefit from a consistent approach to cross border data transfers. The rules remain the same, regardless of the jurisdiction. Complaints can be filed locally, enabling both consumers and businesses to work with local regulators with whom and procedures with which they are familiar. At the same time, organizations will be able to implement consistent privacy policies on a regional or global basis, which in turn will foster greater privacy compliance in general. Consistent policies would allow organizations to benefit from economies related to deployment of uniform policies and allow consumers and regulators the predictability and clarity of uniform policies related to transborder data flows within the region.

Impediments to Cross Border Data Transfers:

The cost of compliance with divergent privacy protection obligations is high, and does not necessarily provide a tangible benefit to data subjects by way of a noticeable improvement to the protection of their privacy. In many cases the processes required to ensure compliance are technically unfeasible, particularly for businesses making comprehensive use of the Internet for the service, benefit and convenience of its customers as well as to rationalize policies and practices to improve compliance and gain potential efficiencies and economies.

Companies whose business involves transferring personal data to other countries with different types of privacy protection face difficulties as privacy protection legislation can forbid these transfers. This can also affect companies operating in the countries to which the data would be transferred. For example, many companies have taken advantage of improvements in the communications infrastructure and the availability of skilled workers in countries outside their main bases of operation to create customer service response centers, such as call centers. This allows companies to provide 24-hour customer service at a competitive price and creates employment around the world. However, for these call centers to operate effectively, they must have access to the customer data of individuals in another country. Restrictions on transferring personal data, or the imposition of onerous burdens on companies, which are disproportionate compared to the interest they are intended to protect, can result in less convenient and competitive customer service, and can also hamper job creation in emerging economies.

While many companies today have comprehensive privacy policies across their organization, without a mechanism to recognize these policies as a legitimate basis upon which to transfer data, they cannot be relied upon with legal certainty for transborder data flows. Any mechanisms that do exist involve lengthy negotiations with a variety of authorities and bureaucratic hurdles that make this option unfeasible for all but the largest companies.

The current global solution, contracts, can be overly burdensome, resulting in thousands of contracts within a single organization.

Verification process for CBPRs' compliance with the APEC Privacy Principles/ Approval Mechanism:

APEC should create a streamlined approach for approving and recognizing an organization's CBPRs. Such an approach would eliminate the cost and uncertainty that arise as a result of the administration of complex contractual arrangements across a global enterprise and would ensure that Privacy Codes recognized in one APEC member economy as consistent with the APEC Privacy Principles are recognized by other APEC economies, thereby providing certainty to businesses that their data transfers are compliant with any privacy obligation within the APEC region. This goal is consistent with the objective identified in the preamble of the Framework, to enable "global organizations that collect, access, use or process data in APEC Member Economies to develop and implement uniform approaches within their organizations for global access to and use of personal information" and advance "international mechanisms to promote and enforce information privacy and maintain the continuity of information flows among APEC economies and with their trading partners." Developing these mechanisms for use on a global basis will encourage effective privacy regimes that realistically reflect the evolving nature of technology and the global marketplace and afford businesses and consumers the benefits of a globally networked world.

As the September 2005 United States paper to APEC proposed, use of Cross Border Privacy Rules would not alter the oversight of the local regulatory authority related to initial collection and domestic use of information. In addition, organizations would still be responsible for complying with the local data protection requirements (e.g., notice, access rights) if any in each of the economies for the collection, use, and disclosure of personal data. In other words, only the subset of the Principles relevant to cross border transfers would need to be incorporated into CBPRs.

The verification process must be flexible to permit a variety of approaches and practices. CBPRs must be tailored to the needs of a particular business or industry sector, taking account of particular challenges and sensitivities, the corporate culture, processes and the organizational structure. USCIB, with its international counterpart, the International Chamber of Commerce, is in the process of developing an accountability framework on which companies can build CBPRs that comply with the APEC Privacy Framework.

Enforcement:

Mechanisms for assuring compliance may vary from one Member Economy to another, depending on the regulatory structure of the Member Economy. A harmonized framework, combined with a mechanism to ensure cross border enforcement, will benefit consumers by

preserving their ability to go to a local self-regulatory enforcement body and/or regulator and improving the ability of the self-regulatory enforcement body and/or regulator to deal with issues outside of its jurisdiction , thus ensuring a uniform level of protection for data transfers across the region in a manner that balances the business need for efficient data flows. As part of its agenda, APEC is considering what the verification process would look like in different regulatory environments and how economies can work together on enforcement issues. Moreover, the mechanism should be able to ensure adherence to the APEC Privacy Principles in a meaningful way without creating unnecessary administrative and bureaucratic obstacles.

In economies that provide significant roles for self regulatory mechanisms, seal programs may be part of an effective mechanism to assure compliance with the APEC Framework. Seal programs already exist in many countries, and act as a mechanism for businesses to assure their customers that privacy protections are observed. A company may chose to join a seal program, implement its privacy principles and practices, allow itself to be audited or monitored by the seal program, and/or have the seal program act as an investigator and enforcer in the event of a customer complaint. This allows the company to display a 'seal of approval' such as a logo on its website or other company materials and provides information to customers making choices in competitive marketplaces. Incorporation of seal programs, as with any possible enforcement mechanism, into the APEC Framework must be done in a flexible manner to allow companies to select the verification and enforcement mechanism that best meets their business need.

Dispute resolution mechanisms are vital to the viability of CBPRs. The international implementation section of the APEC Framework recognizes this important element by foreseeing the need for cross border cooperation in enforcement. Dispute resolution systems do more than resolve disputes. They can also highlight patterns of complaints that an enforcement mechanism can investigate and address. CBPRs could incorporate dispute resolution requirements. By doing so, companies can show they are accountable and also potentially lessen the burden of enforcement on law enforcement agencies.

Enforcement could also be accomplished through ex post facto audits by enforcement authorities in response to the identification of complaint patterns.

Support of the concept of CBPRs by APEC member economies:

For a regional mechanism to be effective, it must be supported by a broad group of APEC member economies. Broad support is also necessary to demonstrate to other regions that this is an effective approach to cross border privacy protection. USCIB is pleased that a study group has been formed within the APEC Privacy Subgroup and a timeline developed that ensures timely implementation of this concept.

Conclusion:

USCIB firmly believes that the introduction of a mechanism to recognize CBPRs in APEC could alleviate the difficulties arising out of the particular uncertainties in determining the legal regime applicable to data processing activities that occur in multiple countries, in particular with respect to on-line transactions, thus facilitating the regional transfer of data necessary for continued trade and investment growth.

We look forward to continuing to work with the Department of Commerce and other members of the US Government APEC Delegation towards this important goal.

Sincerely,

Heather I. Shaw

Director, International Telecommunications and Information Policy